Newton's Method, Galois Theory, and Something You Probably Didn't Know About A_5

David A. Cox

Amherst College

References

- Klein, *Lectures on the Icosahedron*, Teubner, 1884
- Smale, *On the efficiency of algorithm analysis*, Bull. AMS, 1985
- McMullen, *Families of rational maps and iterative root-finding algorithms*, Annals of Math., 1987
- Doyle/McMullen, *Solving the quintic by iteration*, Acta Math., 1989
- Shurman, *Geometry of the Quintic*, Wiley, 1997

Outline

- Newton's Method for Polynomials
- Generally Convergent Iterative Algorithms
- The McMullen Rigidity Theorem
- A Galois Theory of Generally Convergent Iterative Algorithms
- The Doyle/McMullen Theorem and the Quintic
- The Algorithm

Newton's Method for Polynomials

Newton's Method doesn't always converge to a root.

Example: $f(x) = x^3 - 5x$ gives

$$N(x) = x - \frac{f(x)}{f'(x)} = x - \frac{x^3 - 5x}{3x^2 - 5}.$$

N has the 2-cycle $1 \to -1 \to 1 \to$

Can do Newton's Method over $\mathbf{C}$:

Here is Newton's Method for $x^3 - 1$ over $\mathbf{C}$:

Initial values which converge to 1 are shaded black.

Naive Guess:

For a dense open subset of initial values, Newton's Method converges to a root.

Counterexample: Let

- $f(x) = \frac{1}{2}x^3 - x + 1$.
- $N = x - \frac{f(x)}{f'(x)}$.

Then:

- $0 \to 1 \to 0 \to \cdots$ under N.
- $N'(0) = 0$, so attracting 2-cycle.

Hence initial values near 0 or 1 do not converge to a root under Newton's Method.

Generally Convergent Iterative Algorithms

In 1985, Smale asked for an iterative algorithm which:

- is rational in the coefficients of a polynomial, and
- converges generally to a root of the polynomial.

Generally convergent means that for $f = x^n + a_1 x^{n-1} + \cdots + a_n$,

- for $(a_1, \ldots, a_n)$ in a dense open subset of $\mathbf{C}^n$, and
- for z_0 in a dense open set of $\mathbf{C}$,

the algorithm converges to a root of f.

In 1987, McMullen proved that an iterative, generally convergent algorithm doesn't exist when $n \geq 4$.

Also, for $n = 3$, consider

$$f(x) = x^3 + ax + b.$$

Then one can show:

- Newton's Method for $f(x)$ is not generally convergent.
- Newton's Method for

$$\frac{f(x)}{3ax^2 + 9bx - a}$$

is generally convergent.

Definition of a Generally Convergent Iterative Algorithm:

Consider a field K which is:

- a finite extension of $\mathbf{C}(t_1, \ldots, t_n)$, or equivalently,
- the rational function field $\mathbf{C}(V)$ of an irreducible variety V.

(An example is $V = \mathbf{C}^n$.)

Definition: A **rational iterative algorithm** is an element $T \in K(z)$, where z is a coordinate on

$$\mathbf{P}^1 = \mathbf{C} \cup \{\infty\}.$$

Example: For $K = \mathbf{C}(a_1, \ldots, a_n)$ and $V = \mathbf{C}^n$, Newton's Method is

$$N = z - \frac{z^n + a_1 z^{n-1} + \cdots + a_n}{n z^{n-1} + \cdots + a_{n-1}}$$

This is an element of $K(z)$.

Notation: Let $T \in K(z)$. For most $v \in V$, $T_v \in \mathbf{C}(z)$ is defined. Thus $T_v : \mathbf{P}^1 \to \mathbf{P}^1$.

Definition: T is **generally convergent** if $\{T_v^n(z)\}_{n=0}^{\infty}$ converges for (v, z) in a dense open subset of $V \times \mathbf{P}^1$.

The McMullen Rigidity Theorem

Theorem: If T is generally convergent, then for v in a dense open subset of V, the maps T_v are all conjugate under $\mathrm{PGL}(2, \mathbf{C})$.

Example: For $K = \mathbf{C}(t)$, $T_t = z - \frac{z^n - t}{nz^{n-1}}$ is generally convergent. If $\phi(z) = z/a$, then

$$\phi \circ T_t \circ \phi^{-1} = T_{t/a^n}.$$

Note also that $a = \sqrt[n]{t}$ implies

$$T_t = \phi^{-1} \circ f \circ \phi, \ f = z - \frac{z^n - 1}{nz^{n-1}}.$$

This will be useful later.

Corollary: No generally convergent iterative algorithm for general polynomial of degree ≥ 4.

Proof: If such an algorithm existed for a general polynomial of degree n, then the roots would be conjugate under $\mathrm{PGL}(2, \mathbf{C})$.

More precisely, suppose f, g have degree n. If f has roots a_i, then we can find z_i with

$$T_f^n(z_i) \to a_i$$

If we have $\phi \in \mathrm{PGL}(2, \mathbf{C})$ with

$$\phi \circ T_f \circ \phi^{-1} = T_g,$$

then setting $w_i = \phi(z_i)$ implies

$$T_g^n(w_i) \to \phi(a_i)$$

Thus the $\phi(a_i)$ are the roots of g.

But the action $\mathrm{PGL}(2, \mathbf{C})$ on $\mathbf{P}^1$ is only 3-transitive!

A Galois Theory of Generally Convergent Iterative Algorithms

The **output** of T is the set

$$\text{Output}(T)$$

consisting of all $(v, w) \in V \times \mathbf{P}^1$ such that

$$w = \lim_{n\to\infty} T_v^n(z)$$

for an open set of z's. Note that

$$\text{Output}(T) \subset \{(v, w) \mid T_v(w) = w\}.$$

Let $\overline{\text{Output}(T)}$ be the smallest variety containing $\text{Output}(T)$.

Definition: A generally convergent iterative algorithm $T \in K(z)$ is **irreducible** if $\overline{\text{Output}(T)}$ is an irreducible variety. We denote its function field by K_T.

Such a T gives a finite extension

$$K \subset K_T.$$

Let K' be the Galois closure of this extension and set

$$G = \text{Gal}(K'/K).$$

Theorem: (Doyle/McMullen)

If T is as above, then there are:

- $f(z) \in \mathbf{C}(z)$
- $\phi \in \mathrm{PGL}(2, K')$
- $\rho : G \to \mathrm{PGL}(2, \mathbf{C})$ injective

such that:

1) $T = \phi^{-1} \circ f \circ \phi$
2) $\{f^n(z)\}_{n=0}^{\infty}$ converges on a dense open set of $\mathbf{P}^1$

Furthermore:

3) $f \circ \rho(g) = \rho(g) \circ f$ for all $g \in G$.
4) $\phi^g = \rho(g) \circ \phi$ for all $g \in G$.
5) All irreducible generally convergent iterative algorithms arise this way.

Example: Let $K = \mathbf{C}(t)$ and $T = z - \dfrac{z^n - t}{nz^{n-1}}$. Then we have:

$$K_T = K' = \mathbf{C}(\sqrt[n]{t}).$$

Furthermore:

- $f = z - \dfrac{z^n - 1}{nz^{n-1}}$.

- $\phi = \begin{pmatrix} 1/\sqrt[n]{t} & 0 \\ 0 & 1 \end{pmatrix} \in \mathrm{PGL}(2, K')$.

- $G = \{\sigma_i\}$, $\sigma_i(\sqrt[n]{t}) = \zeta_n^i \sqrt[n]{t}$.

- $\rho(\sigma_i) = \begin{pmatrix} \zeta_n^{-i} & 0 \\ 0 & 1 \end{pmatrix} \in \mathrm{PGL}(2, \mathbf{C})$.

Definition: $K \subset L$ is **computable** if there are fields

$$K = K_0 \subset K_1 \subset \cdots \subset K_m$$

such that:

- $L \subset K_m$, and
- There are generally convergent irreducible $T_i \in K_i(z)$ such that $K_{i+1} = (K_i)_{T_i}$ for all i.

Definition: A finite group is called **nearly solvable** if its Jordan-Hölder components are either cyclic or A_5.

The Doyle/McMullen Theorem and the Quintic

Theorem: $K \subset L$ is computable $\iff$ Gal(L'/K) is nearly solvable, $L' =$ Galois closure of $K \subset L$.

Proof: We can assume the Galois group is cyclic or A_5. By the Doyle/McMullen theorem, we need to find f, ϕ, ρ.

Cyclic Case: Done by previous example!

A_5 **Case:** Solve the quintic by iteration. First use Tschirnhaus transformations to reduce to

$$z^5 - 10Cz^3 + 45C^2z - C^2 = 0.$$

This is the **Brioschi resolvent**.

Next project the icosahedron onto S^2 and then map to the plane via sterographic projection. Then consider

$$F(x, y) = x^{11}y + 11x^6y^6 - xy^{11}.$$

This is invariant under the binary icosahedral group and vanishes at the 12 vertices.

Then the rational function

$$f_{11}(z) = -\frac{\frac{\partial F}{\partial y}(z,1)}{\frac{\partial F}{\partial x}(z,1)}$$
$$= -\frac{z^{11} + 66z^6 - 11z}{11z^{10} + 66z^5 - 1}$$

has nice properties:

- f_{11} commutes with A_5.
- The 20 face centers are the critical points of f_{11}.
- f_{11}(face center) = center of antipodal face.

Thus the face centers give ten 2-cycles for f_{11}.

Dynamical Systems Theory $\Rightarrow$ there is a dense open set of $\mathbf{P}^1$ on which

$$\{f_{11}^n(z)\}_{n=0}^{\infty}$$

converges to of the ten 2-cycles.

Then $f = f_{11} \circ f_{11}$ is what we want! It remains to:

- Find ϕ.
- Compute $T = \phi^{-1} \circ f \circ \phi$.
- Relate to Brioschi resolvent.

This gives the following algorithm.

The Algorithm

Define $g(Z,w)$ to be the polynomial:

$$91125Z^6 + (-133650w^2 + 61560w - 193536)Z^5 + (-66825w^4 + 142560w^3 + 133056w^2 - 61440w + 102400)Z^4 + (5940w^6 + 4752w^5 + 63360w^4 - 140800w^3)Z^3 + (-1485w^8 + 3168w^7 - 10560w^6)Z^2 + (-66w^{10} + 440w^9)Z + w^{12}$$

Define $h(Z,w)$ to be the polynomial:

$$(1215w - 648)Z^4 + (-540w^3 - 216w^2 - 1152w + 640)Z^3 + (378w^5 - 504w^4 + 960w^3)Z^2 + (36w^7 - 168w^6)Z$$

To solve $s^5 - 10Cs^3 + 45C^2 s - C^2 = 0$, proceed in five steps:

1) Set $Z = 1 - 1728C$.

2) Compute the rational function

$$T_Z = w - 12\frac{g(Z,w)}{\frac{\partial g}{\partial w}(Z,w)}.$$

3) Iterate $T_Z(T_Z(w))$ on a random starting point until it converges to a limit point w_0. Set $w_1 = T_Z(w_0)$.

4) For $i = 0, 1$ compute

$$\mu_i = \frac{100Z(Z-1)h(Z,w_i)}{g(Z,w_i)}.$$

5) Finally, for $i = 0, 1$, compute

$$s_i = \frac{(9+\sqrt{-15})\mu_i + (9-\sqrt{-15})\mu_{1-i}}{90}.$$

Then s_0 and s_1 are two roots of the Brioschi resolvent!